

Creazione regola Pfsense

Aggiungiamo e configuriamo un nuova interfaccia su Pfsense

Speed and Duplex Default (no preference, typically autoselect) v
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 192.168.50.1 / 24 v

IPv4 Upstream gateway None + Add a new gateway

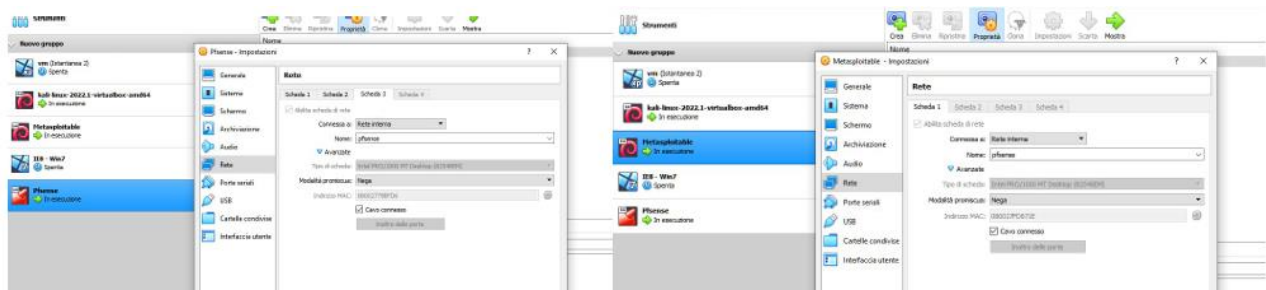
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.
Gateways can be managed by [clicking here](#).

Reserved Networks

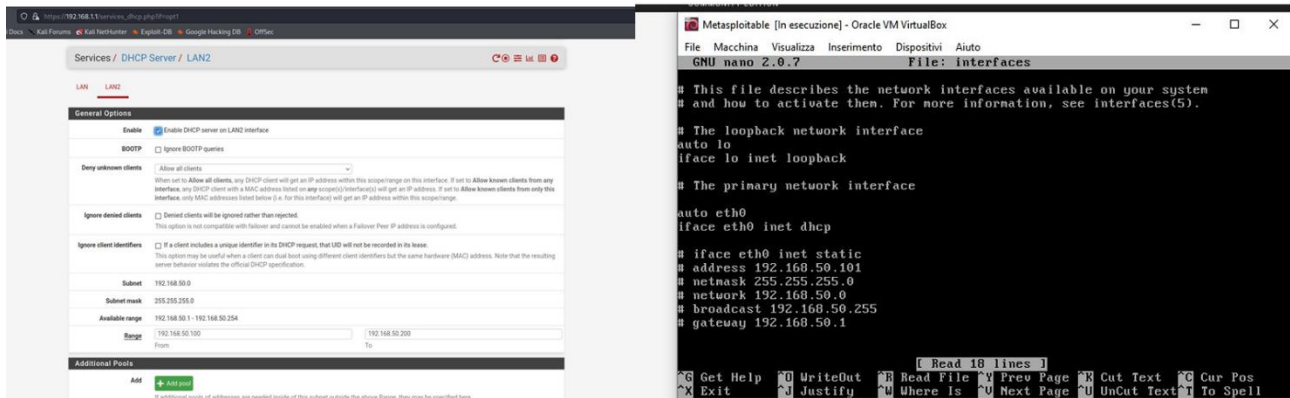
Block private networks and loopback addresses ☐

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a

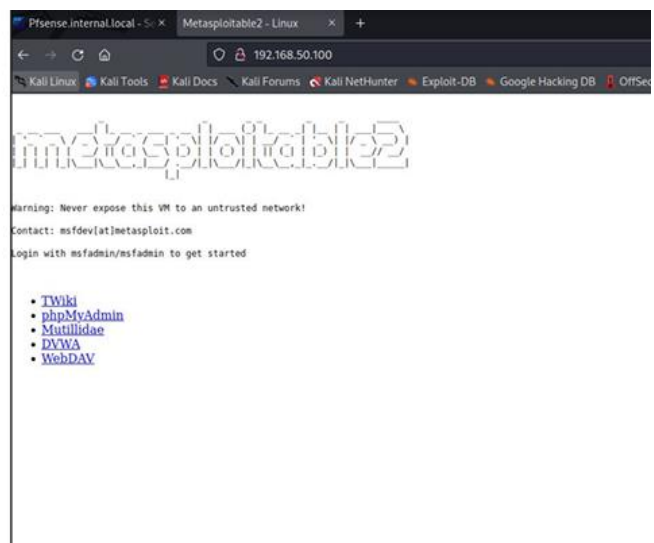
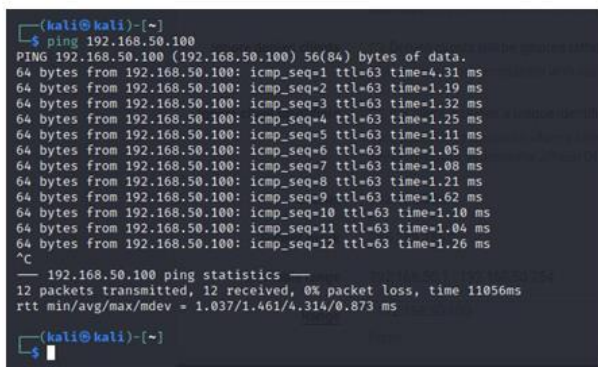
Modifichiamo le impostazioni delle interfacce di Pfsense e Metasploit da virtualbox in modo da averle entrambe su una stessa sottorete che abbiamo chiamato pfsense



Abilitiamo il servizio dhcp sull'interfaccia appena creata (figura a sinistra) e modifichiamo le impostazioni di rete di Metasploitable (al path /etc/network/interfaces) in modo da non utilizzare la configurazione di rete statica come configurato in precedenza



Controlliamo l'ip della macchina Metasploitable e verifichiamo ci sia connettività con la Kali anche verso la DVWA



Creiamo la regola per bloccare il traffico sulla porta 80 da Kali a Metasploitable. Stiamo di fatto rendendo la DVWA non accessibile da Kali. Abilitiamo i log così possiamo vedere il traffico che viene gestito dalla regola

Action	Block		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	TCP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	Single host or alias	192.168.1.100 /
<input type="button" value="Display Advanced"/>			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any .			
Destination			
Destination	<input type="checkbox"/> Invert match	Single host or alias	192.168.50.100 /
Destination Port Range	HTTP (80)	HTTP (80)	
	From	To	
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			
Extra Options			
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).		

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top status bar shows the interface is capturing on eth1. The packet list pane on the left shows a series of packets, with the first packet (No. 1) selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.50.100	TCP	74	40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
2	0.252794082	192.168.1.100	192.168.50.100	TCP	74	40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
3	1.813379382	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
4	1.268813695	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
5	3.829265070	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
6	3.286538176	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
7	5.177621129	PcsCompu_39:7d:fe	PcsCompu_39:9b:90	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
8	5.178182845	PcsCompu_39:9b:90	PcsCompu_39:7d:fe	ARP	60	192.168.1.1 is at 08:00:27:09:9b:90
9	7.422437040	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
10	7.476970973	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
11	14.498684181	fe80:a90:27ff:fe39:f602::1:2	f602::1:2	DHCPv6	166	Information-request XID: 6x8a5a33 CID: 00043c254755bd86d9da8dc6ba2286a9ef
12	15.421916434	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0
13	15.670412997	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 40922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2625019256 Tsecr=0 WS=0

Infine, dai log del Firewall abbiamo la conferma che la nostra regola, che abbiamo chiamato Block DVWA from Kali, sta effettivamente bloccando il traffico da Kali verso la DVWA.

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 2 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✖	Jun 17 12:47:02	LAN	Block DVWA from Kali (1655469329)	192.168.1.100:40026	192.168.50.100:80	TCP:S
✖	Jun 17 12:47:03	LAN	Block DVWA from Kali (1655469329)	192.168.1.100:40028	192.168.50.100:80	TCP:S